REMARKS

Favorable reconsideration and allowance of the claims of the present application, as amended, is respectfully requested.

In the present Office Action, the Examiner reminded applicant to file a certified copy of the priority document in order to claim the benefit of the priority date. Applicants take this opportunity to submit the certified copy in response.

The Examiner then proceeded to object to Claims 1, 7-12 and 15 as comprising various informalities. For instance, in Claims 1, 7-10 and 12 the notation "C" was unclear as it identified two different functions; and, Claim 11 was in improper multiple dependent form with Claim 15 objected to as dependent upon objected Claim 11. In response, applicants have canceled from each of claims 1, 7-10 and 12 the alternative recitation of the use of cryptogram C. Thus, in each of these amended claims, each claim now sets forth provision of a cryptogram calculated by C = the function F(A, c), a cryptogram Y = the function F(X, c) and a cryptogram Z = the function H(a, Y, s). Amending the claims this way provides proper antecedent basis for the later recitation in each claim directed to transmitting cryptograms C, Y and Z to said verifier computers. Respectfully no new matter is being submitted. It should be understood that the recitation of a second cryptogram C (C = the function F(g, c) and a cryptogram Y = the function F(B, c)) was stated in the alternate; so the invention would work with either recitation. New Claims 18-23 are being added dependent upon respective Claims 1, 7-10 and 12 to set forth the alternate reference to the second cryptogram C. Moreover, it is interpreted that in the examples provided in the specification, e.g., page 18, step 3, the function Z is calculated so the obtained C, Y and Z are transmitted to the verifier, irregardless of which set of C and Y cryptograms are

used.

With regard to the rejection of Claim 11 as being in improper multiple dependent form, applicant has amended Claim 11 to incorporate wholly the subject matter of respective Claims 9 and 10, and is thus recast in independent form. Claim 11 respectfully, is now in proper form. The rejection of Claim 15 is obviated due to the amendment do Claim 11.

It is respectfully submitted that the amendments to Claim 1, 7-12 address each of the problems indicated by the Examiner, and the Examiner is respectfully requested to remove the objections in light of these amendments.

The Examiner then proceeded to rejection Claims 1-10, 14-17 under 35 U.S.C. §112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. For instance, the limitations in Claims 1, 8 and 10 recitations of "Z" are allegedly unclear. Further, the word "should" as used in Claims 1, 7-10 and 12 render these claims ambiguous. Further alleged instances of unclear claims in Claims 9 and 14-17 were indicated by the Examiner.

With respect to the Examiner's rejection of Claims 1 –10 and 14-17, applicants have amended each of independent Claims 1, 7-10 and 12 to remove any ambiguity with respect to the recitation of the function "Z". That is, each of these claims has been amended to positively set forth the step of always transmitting cryptograms C, Y and Z (not just C and Y) as previously stated. Thus, there is no longer the ambiguity with respect to function "Z" as being transmitted (and later calculated in the function "A" a function of "Z") as the Examiner interpreted the original recitation of these claims. In light of this clarification, the Examiner is respectfully requested to

reconsider the recitations in Claims 8 and 10 directed to a phrase "are established at the same time" as the Examiner had indicated that this phrase was ignored due to the informalities with respect to the recitation concerning function "Z".

Moreover, Claims 1, 7-10 and 12 have been amended to remove offending language directed to the ambiguous term "should" as in the original filed versions of these claims.

Moreover, Claims 13-17 have been amended to remove allegedly unclear language directed to the ambiguous term "effect" as in the original filed versions of these claims. It is respectfully submitted that Claims 13-17 now set forth more clear and definite subject matter.

Thus, in view of the amendments to Claims 1, 7-10, 12 and 13-17, the Examiner is respectfully requested to withdraw the rejections based on 35 U.S.C. §112, second paragraph.

Further in the Office Action, the Examiner proceeded to reject Claims 1-10, 12-14 and 16-17 under 35 U.S.C. §103(a) as being unpatentable over Schneier reference entitled "Applied Cryptography Protocols, Algorithms and Source Code in C", 2nd Edition, 1996 in view of Trostle (US Patent No. 6,718,467). The Examiner particularly alleges that Schneier teaches the Diffie-Helman's key-exchange algorithm (on page 513) allegedly covers the "calculating" step limitation of Claim 1, e.g., obtaining cryptograms A = the function F(g, a), and B = the function F(g, b) and a cryptogram X = the function F(A, b), where a, b are generated random numbers, and transmitting said cryptograms B and X to said prover computer that determines at the prover computer whether a relation of said cryptogram X = the function F(B, a) has been established. While this may be in accordance with the cited art, e.g., Diffie-

Hellman, this teaching only goes as far as these initial recitations (likewise for amended Claims 7-10 and 12).

However, the Examiner has not directly provided a teaching directed to the further steps recited in each of amended Claims 1, 7-10 and 12 that are performed at the prover computer including: generating a random number c when the relation (X = the function F(B, a)) has been established, and obtaining a cryptogram C = the function F(A, c), a cryptogram Y = the function F(X, c) and a cryptogram Z = a function H(a, Y, s), and transmitting the cryptograms C, Y and Z to the verifier computers; such that the verifier computers establish that a cryptogram Y = the function F(C, b) and a cryptogram A = a function J(v, Y, g, Z) to determine that the relation between the prover computer and the verifier computer is correct.

In this manner, according to the invention as set forth in each of amended Claims 1, 7-10 and 12, will the zero knowledge property for user authentication be workable for multiple connected clients (i.e., verifiers) communicating with the prover computer over an asynchronous network.

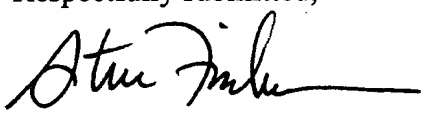
Respectfully, while Trostle teaches mutual authentication, it does not teach the steps described and set forth in each of amended Claims 1, 7-10 and 12. Trostle describes using a password based protocol including a variant of the Diffie-Hellman algorithm for preventing password chaining attack in the first of many exchanges between client and the verifier, and is particularly directed to the innovation of requiring the change of a master password (e.g., col. 6, lines 9-22 of Trostle) in the midst of the communications after performing the first verification to create additional Diffie-Hellman pairs. Trostle, therefore, requires further user interaction by entering an additional password so the client can store a new master key. Respectfully, this is

antithetical to achieving the zero exchange property for user authentication in the manner as performed by the present invention.

Thus, respectfully, the combination of Schneier whether taken alone or in combination with Trostle does not teach the invention as set forth in amended Claims 1, 7-12. Accordingly, the Examiner is respectfully requested to withdraw the rejections of Claims 1-10, 12-14 and 16-17 under 35 U.S.C. §103(a).

In view of the foregoing amendments and remarks, this application is now believed to be in condition for allowance, and a Notice of Allowance is respectfully requested. If the Examiner believes a telephone conference might expedite prosecution of this case, it is respectfully requested that he call applicant's attorney at (516) 742-4343.

Respectfully submitted,



Steven Fischman
Registration No. 34,594

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343
SF:gc